Additional Measures to Bolster the Security of Digital Banking - FAQs

Provides clarifications to some frequently asked questions on the set of additional measures to bolster the security of digital banking that was announced by MAS and ABS on 19 January 2022.

A. Scope

1. **Do the measures apply to corporate banking or private banking customers?**
   The measures announced in the MAS-ABS Statement on 19 January 2022 (Statement) are applicable only to the bank's retail banking business.

   Nonetheless, the bank can assess the applicability of the measures in the Statement and decide if they are relevant for its corporate banking or private banking businesses.

2. **Do the measures apply to non-bank financial institutions?**
   The measures announced in the Statement are applicable only to retail banks.

   Nonetheless, all financial institutions are expected to have in place robust measures to prevent and detect scams, as well as effective incident handling and customer service in the event of a scam. The measures in the Statement can help bolster the security of online interactions with customers. Financial institutions should consider if the measures are relevant to their business.

B. Application of measure in paragraph 3(a) of the Statement - Removal of clickable links in emails or SMS sent to retail customers

1. **Does the removal of clickable links apply to both emails and SMS?**
   All links in emails and SMS to retail customers should be removed.

2. **Is the use of QR codes sent via emails allowed?**
   The use of QR Codes in emails directing customers to websites is not allowed.

3. **Does the removal of clickable links apply to links within e-advices and e-statements?**
   Banks may continue to send password encrypted e-advices and e-statements to customers, provided that any links within are solely for the purpose of providing information to the customer and do not directly result in the customer providing his access codes (*as defined under the E-Payments User Protection Guidelines*), or performing a transfer or payment transaction.

4. **Does the removal of clickable links apply to links (a) containing disclaimers and terms & conditions for banking products, (b) containing information on banking products, (c) containing application forms e.g. resumption of online application, (d) prompting customers to take action or provide confirmation e.g. to facilitate the completion of a customer action, and/or (e) diverting customers to virtual calls or chats?**
   Any form of communication to retail customers by the bank or its representatives in the form of email and SMS should not have clickable links. Emails and SMSes may contain instructions directing customers to the bank's official website or bank app for further information. For example, the email or SMS could indicate the keyword to be entered in the search bar of a bank's official website to help customers quickly find the relevant information.

However, clickable links may be included in an email or SMS if both of the following criteria are met:

(i) The customer is expecting to receive the email or SMS from the bank; and
(ii) The contents in the link are solely for the purpose of providing information to the customer and does not directly result in the customer providing his access codes (*as defined under the E-Payments User Protection Guidelines*), or performing a transfer or payment transaction.

Signing up to a bank's general mailing list would not be considered fulfilment of 4(i). However, subscription to a specific newsletter where a customer is informed of the frequency of email delivery would fulfil 4(i)

5. **Does the removal of clickable links apply to links sent by the bank's partners (on the bank's behalf) to its customers?**
Any form of communication to retail customers by the bank's partners (sent in the name of the bank) in the form of email and SMS should not have clickable links, but instead contain instructions to direct customers to the bank's official website or bank app for further information.

6. **Phone numbers (e.g. banks' hotline numbers) are usually included in banks' SMS alerts. While banks are not sending the phone numbers as clickable, the operating system of mobile phones may make the phone numbers clickable. Does the removal of clickable links apply to phone numbers in SMS?**
Phone numbers (including both numeric and alphanumeric permutations of phone numbers e.g. 1800-2222265 or 1800-ABCBANK) should be removed from SMSes, regardless of whether the phone numbers are clickable.

The bank's SMS alerts may contain instructions directing customers to the bank's official website or other legitimate sources that indicate the bank's hotline information, such as the bank's ATMs, credit and debit cards.

C. Application of measure in paragraph 3(b) of the Statement - Threshold for funds transfer transaction notifications to customers to be set by default at $100 or lower

1. **In implementing the measure above, can banks allow customers to raise the default threshold for such notifications?**
While banks should lower the default notification alert thresholds for fund transfers to an amount that is S$100 or lower, customers are allowed to subsequently change the default thresholds to cater to their personal preferences. Banks should highlight the risks of doing so to their customers and should send a notification of the change to the customer.

D. Application of measure in paragraph 3(c) of the Statement - Delay of at least 12 hours before activation of a new soft token on a mobile device

1. **Does this measure imply that a 12-hour buffer is required after the activation of a new soft token before making any transactions can be performed? If so, does this buffer apply to all transactions?**
Following the request to activate a soft token on a new mobile device, no high-risk transactions/changes that require soft token signing should be allowed within at least the first 12 hours unless there is a non-straight through process, which is equivalent to a cooling period, used to activate the soft token e.g. registration code to activate a new soft token is sent to customer via postal mail which will provide at least a 12-hour buffer before

the new soft token can be activated. A customer's soft token should reside only in one mobile device at any given time.

Examples of such high-risk transactions/changes may include, but are not limited to, adding of payee, increasing transaction limits, updating of mobile number, email and mailing address, and high value fund transfers.

E. Application of measure in paragraph 3(e) of the Statement - Additional safeguards, such as a cooling-off period before implementation of requests for key account changes such as in a customer's key contact details

1. **Does this measure imply that a cooling-off period is required before making changes to the customer's key contact details? Would a non-straight through process (STP) that takes a couple of days to complete be acceptable? Will putting in place a reasonable time buffer before allowing changes to the customer's key contact details after activation of a new soft token on a mobile device be acceptable?**

   Both implementing a non-STP process or putting in place a time buffer of at least 12 hours are possible safeguards. Other possible safeguards may include transaction blocks. The measure allows banks to put in place relevant measures relating to the request for key account changes, and it is not confined to the example of a cooling-off period.